VZCZCXRO0531
RR RUEHAG RUEHAO RUEHAP RUEHAST RUEHAT RUEHBC RUEHBI RUEHBL RUEHBZ
RUEHCD RUEHCHI RUEHCI RUEHCN RUEHDA RUEHDBU RUEHDE RUEHDF RUEHDH
RUEHDT RUEHDU RUEHED RUEHEL RUEHFK RUEHFL RUEHGA RUEHGD RUEHGH RUEHGI
RUEHGR RUEHHA RUEHHM RUEHHO RUEHHT RUEHIHL RUEHIK RUEHJO RUEHJS RUEHKN
RUEHKR RUEHKSO RUEHKUK RUEHKW RUEHLA RUEHLH RUEHLN RUEHLZ RUEHMA
RUEHMC RUEHMJ RUEHMR RUEHMRE RUEHMT RUEHNAG RUEHNEH RUEHNG RUEHNH
RUEHNL RUEHNP RUEHNZ RUEHPA RUEHPB RUEHPD RUEHPOD RUEHPT RUEHPW RUEHQU
RUEHRD RUEHRG RUEHRN RUEHROV RUEHRS RUEHSK RUEHSL RUEHTM RUEHTRO
RUEHVC RUEHVK RUEHYG
DE RUEHC #8372/01 2371256
ZNR UUUUU ZZH
R 251238Z AUG 09
FM SECSTATE WASHDC
TO ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE
RUEHTRO/AMEMBASSY TRIPOLI 9274

UNCLAS SECTION 01 OF 02 STATE 088372

SIPDIS

E.O. 12958: N/A
TAGS: CASC CPAS KFRD CPPT CVIS
SUBJECT: LEXISNEXIS GUIDANCE ON IDENTITY THEFT

¶1. When it comes to identity theft, it is often difficult to interpret results using LexisNexis. Many of the same factors that indicate identity theft can simply be a mistake or a legitimate association that is difficult to spot. Below are some guidelines to help consular officers interpret the data and suggestions on actions to take.

¶2. CA's access to LexisNexis includes U.S. records only. While it is often useful for research on persons who have been in the United States for extended periods of time, whether or not they are U.S. citizens, it is important to remember that LexisNexis does not contain information from outside the United States.

¶3. Remember that LexisNexis identifies only associations, not ownership. The comprehensive reports in LexisNexis do not indicate who specifically has a certain Social Security Number (SSN) or who specifically is using a certain Social Security Number. LexisNexis is a data aggregator which associates different data points, so overlap with more than one identity is unavoidable. It is therefore not only possible, but common, for roommates or relatives to be associated with one anothers' SSNs.

¶4. As a result, it is possible for a SSN association to be a product of nearly any situation. For example, an associated SSN can come from a shared address, even an address associated in error. Often, a fair amount of research is required to determine which associations are meaningful. Several tools are useful in this endeavor.

¶5. Relavint: The Relavint visual mapping tool can be very helpful in noting where identities are associated with one another. The Relavint icon is immediately next to the order report icon where search results are displayed. Relavint may make some connections automatically that the human eye does not see. You may notice, for example, that two people share an association with a common address or car registration.

¶6. Address History: Multiple, incomplete, and/or gaps in address may suggest identity theft. When a SSN is being used by more than one person, it may cause the information aggregator to list more than one address for a person during a distinct period of time, or to have gaps where there is no address at all. Alternately, it is possible that the history will display a series of address moves back and forth beween two addresses in relatively quick succession. This is because the aggregator is receiving conflicting information and gets "confused."

¶7. Conflicting information that gives the aggregator problems is often a sign that two people are using the same identity. For example, a person could show a consistent address history in New Jersey since 1970, but for the period 2003-present, shows addresses in both New Jersey and in Utah. This may suggest that a second person in Utah is using the person's SSN. If an individual has a complete address history with little overlap, this suggests that identity theft is not an issue.

¶8. Vastly Different SSNs: If an individual has more than one SSN and the numbers clearly have no relation to one another, this is a possible indication of identity theft. However, individuals are often associated if they have similar SSNs due to data entry errors on the part of credit agencies. For example, consider one individual with two SSNs: 333-33-3339 and 333-33-3336. While we cannot rule out identity theft, "9" and "6" are extremely close together on a numeric keypad, and this kind of data entry error is common.

¶9. Source Documents: Identity information in LexisNexis is based on source documentation that it is able to collect or purchase. The fewer source documents listed at the bottom of a LexisNexis report, the better the chance that, if there are multiple identities tied to one SSN, it is a mistake. For example, let's say that an SSN is attached to two identities: the first identity has a long, well developed, and complete address history with 25 source documents, and the second identity has a location history that covers only a couple of months. In all likelihood, the second identity was mistakenly associated with the first.



While identity theft cannot be ruled out completely, when someone tries to steal an identity, that person will likely stick with the identity for an extended period of time (versus abruptly giving it up after a short time) and more source documents associated with that stolen identity would have been generated. Always keep in mind that since LexisNexis is a data aggregator, identity fraud is more likely in a case where someone has two completely different SSNs, multiple simultaneous addresses during the last several years, and no visible connections in Relavint, versus someone who simply has two SSNs associated with his or her name.

¶10. Using Advanced Person Search: The Office of Fraud Prevention Programs (CA/FPP) suggests always starting your search in LexisNexis using the "advanced person search" option. The "advanced person search" option presents the data in a much more coherent and easy to read manner than the "regular person search" option. The "advanced person search" option also attempts to limit a SSN to the actual identity by using "smart" computer technology. A "regular person search" presents information in individual record form, which can be useful when trying to determine where the data came from.

¶11. PIERS: LexisNexis is most powerful when used in combination with the Passport Information Electronic Records System (PIERS). For example, information from passport applications can be entered into the "advanced person search" in LexisNexis to determine if the application data generally agrees with what is found in LexisNexis. If extra or different SSNs are listed, those SSNs can be searched using the SSN search function in PIERS. This type of search can determine if an individual is applying for passports with more than one SSN, or if multiple people are using the same SSN.

¶12. Suggested Actions When Identity Theft is Indicated:

Don't panic! It is extremely common to find multiple persons associated with a SSN in LexisNexis, or for multiple SSNs to be associated with one person. This is usually not a sign of identity theft. The following actions are suggested:

a. Go over the record again and try to determine if any appropriate associations exist.

b. Compare the individual's address history in PIERS with their address history in LexisNexis. If the two databases more or less mirror each other, identity theft is probably not indicated. If they are totally different, this is of concern.

c. Contact your liaison officer in CA/FPP to help with the analysis.

If identity theft is probably indicated:

a. Refer the case to your Assistant Regional Security Officer (ARSO-I) or Regional Security Office (RSO) if you suspect your applicant has stolen an identity.

b. Refer the case to your ARSO-I or RSO (and notify your CA/FPP liaison) if you suspect your applicant is the victim of identity theft. Do NOT inform the applicant. It is nearly impossible to conclusively prove identity theft using LexisNexis.

c. In any case where a SSN may have been compromised, inform your Social Security Administration representative at post.
CLINTON